REMARKS/ARGUMENTS:

Claims 1-23 are pending in this Application, as new claims 9-22 are added by this Amendment. In the Office Action dated September 28th, 2004, the Examiner has objected to the specification as associating reference number 50 with two different terms, has objected to the drawing Figures 1 and 2 as including reference numbers not in the written description (or alternatively objected to the written description as not reciting reference numbers in the drawings), has objected to claims 1, 4 and 8 as lacking proper indentation, and has objected to claims 1, 4, and 8 for reciting the term "capable of". Additionally, the Office Action rejects claims 1-8 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,167,513 to Inoue et al (hereinafter, Inoue). Those objections/rejections are addressed below in turn.

The written description is amended at page 2 to eliminate association of the reference number 50 with the Fig. 1 component AuC. Spelling corrections are also made.

The drawing Figures 1 and 2 are amended and replacement sheets containing the amendments are in the Appendix attached hereto, which further includes annotated drawing sheets. In Figure 1, the reference number 70 is deleted. In Figure 2, the reference number 170 is deleted.

Claims 1, 4 and 8 as presented herein are indented to more clearly parse their separate elements. Indentation is modified in other claims also. It is noted that the change to indentation is not set apart by underlining, strikethroughs, or a parenthetical as to currently amended claim status, as indentation changes are not seen as claim amendments.

With regard to the asserted informalities, the Examiner asserted that, in order to avoid rendering claims 1, 4, and 8 indefinite, the term "capable of" should be corrected. Applicants respectfully disagree and submit that the term "capable of" is definite. Nonetheless, in order to further prosecution, Applicants have modified the term "capable of being" to "configured to be." Applicants request the objection to claims 1, 4, and 8 be withdrawn.

Claims 1, 4 and 8 are rejected as anticipated by Inoue. Claim 1 recites in relevant part:

AMENDMENTS TO THE DRAWINGS:

Sheets 1 and 2 of the drawings have been amended. The two enclosed replacement sheets replace the originally filed drawing sheets. Two annotated sheets are also provided.

> "means for selecting one of said separate ciphering parameters for ciphering communications between said user equipment and said at least two of said plurality of core networks in said access network"

The term separate ciphering parameters necessarily means at least two ciphering parameters. This element is present in each of the independent claims 1, 4, 8, 9 and 15, in nearly identical language. The Office Action asserts that this element is anticipated by Inoue.

Inoue discusses in detail how to combine Mobile IP with IP Security and various network operating policies (see, for example, col. 4, lines 5-30). Figure 3, to which the Examiner is referring to, shows a situation, where the home agent HA is in the home network 1a, the mobile computer MN is in the network 1b, and the correspondent host CH is in the network 1c. In this situation, the mobile computer MN may simultaneously communicate with the home agent HA and the correspondent host CH in two different networks.

Inoue provides only a very basic teaching about the authentication or encryption keys. It states that both encryption/authentication parties need to know the key used in the encryption/authentication or information used for generating the key used in the encryption/authentication. This is generally well known in the art of encryption and authentication.

As examples of the teaching of Inoue regarding encryption/authentication keys, information for obtaining an authentication/encryption key may be in the KEY information header of a packet. Authentication or encryption keys may be generated from a packet processing key (col. 12, lines 33-36). In this case the KEY information header carries information about a packet processing key encrypted by a master key shared by the encryption/authentication parties. A master key to be shared by the two parties can be generated by the exchange of a secret key or a key derivation algorithm involving the public and private keys of the two parties (col. 13, lines 26-31). If needed, the KEY information header contains also information about the authentication or encryption algorithm (col. 12, lines 37-40).

In summary, Inoue may be considered to provide teaching on a mobile computer MN in a network 1b simultaneously in communication with a home agent HA in a network 1a and a correspondent host CH in a network 1c. Regarding the keys for encrypting or authenticating communications, Inoue teaches only that the two end points both need to know the key used for the encryption or authentication.

Inoue is completely silent about selecting a same encryption/authentication key for a number of endpoints (or networks). The claimed invention is therefore novel in view of the disclosure of Inoue.

In accordance with the general teaching of prior art, an encryption key for a first endpoint is selected independently from an encryption key for a second endpoint. Inoue cannot therefore be considered to render the claimed invention obvious.

Liu seems to discuss a number of simultaneous calls or connections, instead of a single call/connection at a time. Liu seems not to refer to security parameters transmitted between core and access networks.

Jonsson seems to discuss how a user may be reachable via a number of access networks, calls to and from the user being connected via an intermediary party. There seems to be no indication of a number core networks or of co-ordination of security parameters used in the access networks.

The claimed invention has, furthermore, the following advantages.

When the access network selects the ciphering parameter to be used for ciphering communications between user equipment and core networks, the access network can access ciphered signaling messages. If more than one ciphering parameters are used, the access network may not be able to access any or some ciphered signaling messages. It may therefore be difficult to manage the resources in the access network properly.

When the ciphering control functionality is provided in the access network, the access network resource control and ciphering control functionality may be relocated together in

a handover. This is easier than relocating access network resource control independently of relocation of ciphering control.

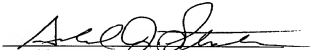
Ciphering of communications to and from a user equipment is also easier in general, when one ciphering parameter is used. Otherwise there would be need to keep track of different ciphering parameters relating to different endpoints.

The claimed invention may also improve security. Consider that a first ciphering parameter is used for an existing communication relating to a first core network. When a second core network provides a second ciphering parameter, and this second parameter is selected for use, this second ciphering parameter may be taken into use also for the existing communication relating to the first core network. This is discussed on page 6, lines 26-30 and Figure 4 shows an example.

As a summary, none of the cited references discloses selecting one ciphering parameter from at least two separate ciphering parameters provided by at least two core networks for use between user equipment and the at least two core networks. Furthermore, the claimed invention has advantages over the cited prior art. We therefore believe that the invention is non-obvious.

The above arguments apply equally to each independent claim, given the similarity of the relevant claim language. In light of the above, the Applicant respectfully requests the Examiner to re-consider and withdraw all claim rejections over Inoue. Further, the Applicant requests the Examiner enter the amended drawings in the record, and withdraw as moot the objections to the drawings, the specification, and terminology in claims 1, 4 and 8. The Applicant invites the Examiner to resolve any remaining matters with the undersigned representative via teleconference, where the Examiner deems it appropriate.

Respectfully submitted:



Gerald J. Stanton
Reg. No.: 46,008

January 14, 2004
Date

Customer No. 29683
HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212
Phone: (203) 925-9400
Facsimile: (203) 944-0245
Email: gstanton@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

January 14, 2004
Date

Ann Okrentowich
Ann Okrentowich

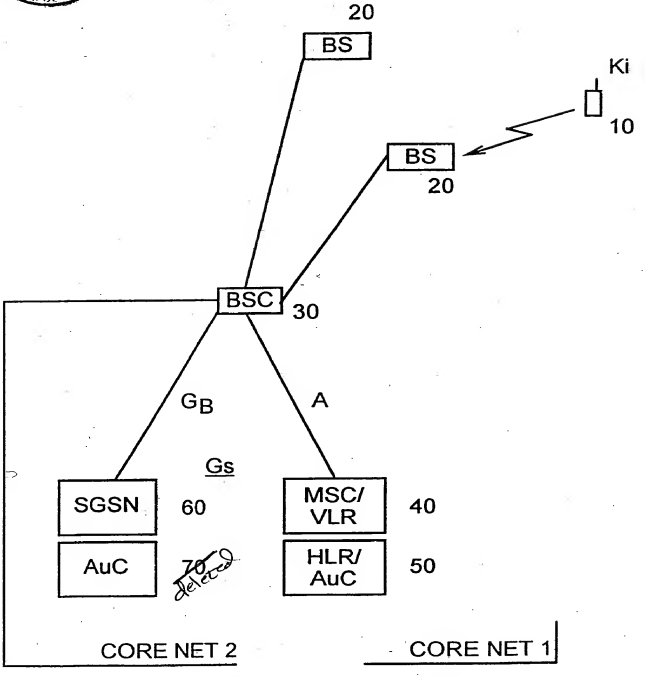


FIGURE 1

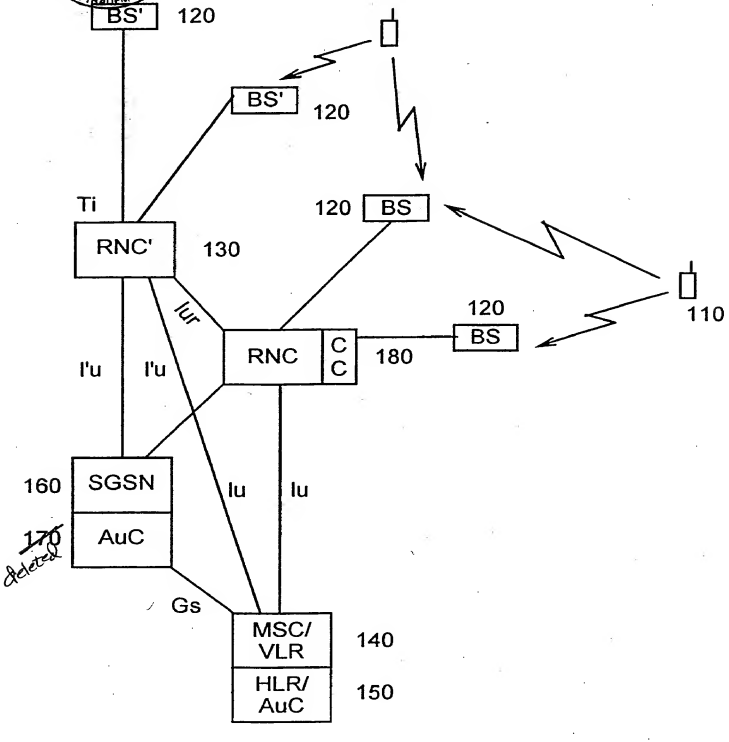


FIGURE 2